UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

LINDABETH RIVERA, on behalf of herself and all others similarly situated, Plaintiff, v. GOOGLE INC., Defendant.	Civil Action No. 1:16-cv-02714 (JURY TRIAL DEMANDED)

FISRT AMENDED CLASS ACTION COMPLAINT

Plaintiff Lindabeth Rivera ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint for violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the "BIPA"), against Google Inc. ("Google"), and alleges as follows based on personal knowledge as to herself, on the investigation of her counsel and the advice and consultation of certain third-party agents as to technical matters, and on information and belief as to all other matters, and demands trial by jury:

NATURE OF ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Google in collecting, storing and using Plaintiff's and other similarly situated individuals' biometric identifiers[1] and biometric information[2] (collectively, "biometrics") without informed written consent, in direct violation of the BIPA.

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA and "face geometry," among others.

[2] "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier used to identify an individual.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometrics – particularly in the City of Chicago, which was recently selected by major national corporations as a "pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias" (740 ILCS 14/5(b)) – the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that a private entity like Google may not obtain and/or possess an individual's biometrics unless it: (1) informs that person in writing that biometric identifiers or information will be collected or stored, *see id.*; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used, *see id.*; (3) receives a written release from the person for the collection of her or her biometric identifiers or information, *see id.*; and (4) publishes publically available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a).

4. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of the BIPA, Google is actively collecting, storing, and using – without providing notice, obtaining informed written consent or publishing data retention policies – the biometrics of thousands of unwitting individuals throughout the country whose faces appear in photographs uploaded to Google Photos in Illinois.

5. Specifically, Google has created, collected and stored, in conjunction with its cloud-based "Google Photos" service, millions of "face templates" (or "face prints") – highly detailed geometric maps of the face – from millions of individuals, many thousands of whom are not even enrolled in the Google Photos service. Google creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in photos taken on Google "Droid" devices and uploaded to the cloud-based Google Photos service. Each face template that Google extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person.

6. Plaintiff brings this action individually and on behalf of all others similarly situated to prevent Google from further violating the privacy rights of individuals not enrolled in Google Photos, and to recover statutory damages for Google's unauthorized collection, storage and use of these unwitting non-users' biometrics in violation of the BIPA.

PARTIES

7. Plaintiff is, and has been at all relevant times, a resident and citizen of Chicago, Illinois. Plaintiff is not, and has never been, an owner or user of a Google Droid device. Plaintiff is not, and has never been, a Google Photos account holder or user of the Google Photos service.

8. Google is a Delaware corporation with its headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Accordingly, Google is a citizen of the states of Delaware and California. Google is also registered to do business in Illinois (No. 65161605) and maintains an office in Cook County, Illinois.

JURISDICTION AND VENUE

9. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA"), because: (i) the proposed class consists of well over 100 members; (ii) the parties are minimally diverse, as members of the proposed class, including Plaintiff, are citizens

of a state different from Google's home states; and (iii) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interests and costs. There are likely hundreds of thousands of individuals who had their photos uploaded to Google Photos from within Illinois, even though they are not users of Google Photos. The estimated number of non-Google Photo users who were impacted by Google's conduct multiplied by the BIPA's statutory liquidated damages figure ($5,000.00 for each intentional or reckless violation and $1,000.00 for each negligent violation) easily exceeds CAFA's $5,000,000.00 threshold.

10. Google is subject to personal jurisdiction in Illinois because the photos of Plaintiff giving rise to this lawsuit (*i.e.*, the photos from which the illegal face templates were derived) were captured on, and uploaded in Illinois to Google Photos by, a Google Droid device that was shipped by Google into Illinois and purchased by a Google Photos user in Illinois. Google is also subject to personal jurisdiction in Illinois because it targets its facial recognition technology towards millions of its users who are residents of Illinois, because Plaintiff and tens of thousands of other non-Google Photo users had their biometric identifier(s) collected by Google from photographs uploaded in Illinois and tagged by Google users residing in Illinois, and because it maintains an office in Cook County, Illinois.

11. Venue is proper in this District because Plaintiff resides in this District, and because the claims alleged in this lawsuit arose in large part in this District.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

12. "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific "biometric identifiers" (*i.e.*, details about the face's geometry as determined by facial points and

contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a "face template database." If a database match is found, an individual may be identified.

13. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[3] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[4]

14. The Federal Trade Commission ("FTC") has raised similar concerns, and recently released a "Best Practices" guide for companies using facial recognition technology.[5] In the guide, the Commission underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs.

15. As explained below, Google failed to obtain consent from unwitting non-users when it introduced its facial recognition technology. Not only do the actions of Google fly in the face of FTC guidelines, they also violate the privacy rights of Illinois residents.

---

3 *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf (last visited Mar. 1, 2016).

4 *Id.*

5 *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (last visited Mar. 1, 2016).

II. Illinois's Biometric Information Privacy Act

16. In 2008, Illinois enacted the BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. The BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[6] or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

740 ILCS 14/15 (b).

17. Section 15(a) of the BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

18. As alleged below, Google's practices of collecting, storing and using unwitting non-users' biometric identifiers and information derived from photographs uploaded in Illinois without informed written consent violate all three prongs of § 15(b) of the BIPA. Google's failure to provide a publicly available written policy regarding their schedule and guidelines for the

[6] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (i.e., facial data obtained through facial recognition technology). *See* 740 ILCS 14/10.

retention and permanent destruction of non-users' biometric information also violates § 15(a) of the BIPA.

III. Google Violates Illinois's Biometric Information Privacy Act

19. In May 2015, Google announced the release of its photo sharing and storage service called Google Photos. Users of Google Photos upload millions of photos per day, making photographs a vital part of the Google experience.

20. The Google Photos app, which comes pre-installed on all Google Droid devices, is set by default to automatically upload all photos taken by the Droid device user to the cloud-based Google Photos service. Users can also connect other devices to Google Photos to upload and access photos on the cloud-based service.

21. Unbeknownst to the average consumer, and in direct violation of § 15(b)(1) of the BIPA, Google's proprietary facial recognition technology scans each and every photo uploaded to the cloud-based Google Photos for faces, extracts geometric data relating to the unique points and contours (*i.e.,* biometric identifiers) of each face, and then uses that data to create and store a template of each face – all without ever informing anyone of this practice.[7]

22. The cloud-based Google Photos service uses these face templates to organize and group together photos based upon the particular individuals appearing in the photos. This technology works by comparing the face templates of individuals who appear in newly-uploaded photos with the facial templates already saved in Google's face database. Specifically, when a Google Photos user uploads a new photo, Google's sophisticated facial recognition technology creates a template for each face depicted therein, without consideration for whether a particular face belongs to a Google Photos user or unwitting non-user, and then compares each template against

[7] Google holds several patents covering its facial recognition technology that detail its illegal process of scanning photos for biometric identifiers and storing face templates in its database without obtaining informed written consent.

Google's face template database. If there is a match, then Google groups the photo from which the newly-uploaded face template was derived with the previously uploaded photos depicting that individual.

23. These unique face templates are not only collected and used by Google Photos to identify individuals by name, but also to recognize their gender, age, and location. Accordingly, Google also collects "biometric information" from non-users. *See* 740 ILCS 14/10.

24. In direct violation of §§ 15(b)(2) and 15(b)(3) of the BIPA, Google never informed unwitting non-users who had their face templates collected of the specific purpose and length of term for which their biometric identifiers or information would be collected, stored and used, nor did Google obtain a written release from any of these individuals.

25. In direct violation of § 15(a) of the BIPA, Google does not have written, publicly available policies identifying their retention schedules, or guidelines for permanently destroying non-users' biometric identifiers or information.

IV. Plaintiff's Experience

26. Plaintiff does not have, and has never had, a Google Droid device or a Google Photos account. Plaintiff does not use, and has never used, a Google Droid device or a Google Photos account.

27. Over the course of approximately the past year, a Google Photos user who resides in Illinois took approximately eleven (11) photos of Plaintiff in the state of Illinois using a Google Droid device that Google shipped into, and was purchased in, the state of Illinois. The Google Droid device on which these photos of Plaintiff were captured automatically uploaded the photos to the cloud-based Google Photos service. These photos were all uploaded to the cloud-based Google Photos service while the Google Droid device was located in the state of Illinois and assigned an Illinois-based IP address.

28. Immediately upon upload to the cloud-based Google Photos storage service, Google analyzed these photos by automatically locating and scanning Plaintiff's face, and by extracting geometric data relating to the contours of her face and the distances between her eyes, nose, and ears – data which Google then used to create a unique template of Plaintiff's face.

29. The resulting unique face template was used by Google to locate and group together all photos depicting Plaintiff for organizational purposes.

30. Plaintiff's face template was also used by Google to recognize Plaintiff's gender, age, race, and location.

31. Plaintiff never consented, agreed or gave permission – written or otherwise – to Google for the collection or storage of her unique biometric identifiers or biometric information.

32. Further, Google never provided Plaintiff with nor did she ever sign a written release allowing Google to collect or store her unique biometric identifiers or biometric information.

33. Likewise, Google never provided Plaintiff with an opportunity to prohibit or prevent the collection, storage or use of her unique biometric identifiers or biometric information.

34. Nevertheless, when a Google Photos user took and uploaded photos of Plaintiff from within the state of Illinois, Google located Plaintiff's face in the photos, scanned Plaintiff's facial geometry, and created a unique face template corresponding to Plaintiff, all in direct violation of the BIPA.

CLASS ALLEGATIONS

35. **Class Definition**: Plaintiff brings this action pursuant to Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All non-users of the Google Photos service who had their biometric identifiers, including scans of face geometry, collected, captured,

received, or otherwise obtained by Google from photographs uploaded within the state of Illinois.

The following are excluded from the Class: (1) any Judge presiding over this action and members of her or her family; (2) Google, Google's subsidiaries, parents, successors, predecessors, and any entity in which Google or its parent has a controlling interest (as well as current or former employees, officers and directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Google's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

36. **Numerosity**: The number of persons within the Class is substantial, believed to amount to thousands of persons. It is, therefore, impractical to join each member of the Class as a named Plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation.

37. **Commonality and Predominance**: There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any class member include, but are not limited to, the following:

(a) whether Google collected or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

(b) whether Google properly informed Plaintiff and the Class that it collected, used, and stored their biometric identifiers or biometric information;

(c) whether Google obtained a written release (as defined in 740 ILCS 1410) to collect, use, and store Plaintiff's and the Class's biometric identifiers or biometric information;

(d) whether Google developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of their last interaction, whichever occurs first;

(e) whether Google used Plaintiff's and the Class's biometric identifiers or biometric information to identify them; and

(f) whether Google's violations of the BIPA were committed intentionally, recklessly, or negligently.

38. **Adequate Representation**: Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Neither Plaintiff nor her counsel has any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff is able to fairly and adequately represent and protect the interests of such a Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class or additional claims as may be appropriate.

39. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the

parties and of the court system and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with the BIPA.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

40. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

41. The BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b) (emphasis added).

42. Google is a Delaware corporation and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

43. Plaintiff and the Class members had their "biometric identifiers," including scans of face geometry, collected, captured, received, or otherwise obtained by Google from photographs that were uploaded to Google Photos from within the state of Illinois. *See* 740 ILCS 14/10.

44. Plaintiff and the Class members are individuals who had their "biometric information" collected by Google (in the form of their gender, age and location) through Google's collection and use of their "biometric identifiers."

45. Google systematically and automatically "collect[ed], capture[d], purchase[d], receive[d] through trade, or otherwise obtain[ed]" Plaintiff's and the Class members' biometric

identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

46. In fact, Google failed to properly inform Plaintiff or the Class in writing that their biometric identifiers and/or biometric information were being "collected or stored" on Google Photos, nor did Google inform Plaintiff or the Class members in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2).

47. In addition, Google does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiff or the Class members, as required by the BIPA. *See* 740 ILCS 14/15(a).

48. By "collect[ing], captur[ing], purchas[ing], receiv[ing] through trade, or otherwise obtain[ing]" Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Google violated the right of Plaintiff and each Class member to keep private these biometric identifiers and biometric information, as set forth in the BIPA.

49. On behalf of herself and the proposed Class members, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Google to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) statutory damages of $5,000.00 for the intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20 (2), or alternatively, statutory damages of $1,000.00 pursuant to 740 ILCS 14/20(1) if the Court finds that Google's violations were negligent; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Lindabeth Rivera, on behalf of herself and the proposed Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class, and appointing her counsel as Class Counsel;

B. Declaring that Google's actions, as set out above, violate the BIPA, 740 ILCS l4/1, *et seq.*;

C. Awarding statutory damages of $5,000.00 for each and every intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000.00 pursuant to 740 ILCS 14/20(1) if the Court finds that Google's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an order requiring Google to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

50. Plaintiff demands a trial by jury for all issues so triable.

Dated: March 27, 2016

Respectfully submitted,

By: */s/Frank S. Hedin*
CAREY RODRIGUEZ
MILIAN GONYA, LLP
David P. Milian*

dmilian@careyrodriguez.com
Frank S. Hedin*
fhedin@careyrodriguez.com
1395 Brickell Avenue, Suite 700
Miami, Florida 33131
Telephone: (305) 372-7474
Facsimile: (305) 372-7475

Katrina Carroll
kcarroll@litedepalma.com
Kyle A. Shamberg
kshamberg@litedepalma.com
Lite DePalma Greenberg, LLC
211 West Wacker Drive, Suite 500
Chicago, Illinois 60606
Telephone: (312) 750-1265

AHDOOT & WOLFSON, PC
Robert Ahdoot*
radhoot@ahdootwolfson.com
Tina Wolfson*
twolfson@ahdootwolfson.com
Brad King*
bking@ahdootwolfson.com
1016 Palm Avenue
West Hollywood, California 90069
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

**Pro Hac Vice Application Forthcoming*

Counsel for Plaintiff and the Putative Class